REMARKS

Claims 1, 3, 10, and 15 are amended, no claims are canceled, and no claims are added; as a result, claims 1-15 are now pending in this application.

No new matter has been introduced through the amendments to claims 1, 3, 10, and 15. Support for the amendments to claims 1, 3, 10, and 15 may be found throughout the specification, including but not limited to the specification at page 2, lines 16-19.

§102 Rejection of the Claims

Claims 1-15 were rejected under 35 U.S.C. § 102(e) for anticipation by Graunke et al. (U.S. 5,991,399, hereinafter "Graunke"). Applicant respectfully traverses the rejection of claims 1-15.

Applicant maintains, for at least the reasons provided in Applicant's previous response,[1] that claims 1-15 are not anticipated by Graunke, and that the Final Office Action fails to show how Graunke discloses all of the claimed subject matter included in claims 1-15. Therefore, Applicant maintains that the Final Office Action fails to meet its burden for establishing a *prima facie* case of anticipation with respect to claims 1-15.

An important advantage of the claimed invention is that it makes it possible to provide an interface between a secure device and a content player without specific knowledge beforehand of the protocol required by the specific secure device used (*See* e.g. page 5 lines 10-13 of Applicant's specification). As such, the invention allows content protection technology to be adapted and to maintain interoperability with existing technology used in present consumer equipment (*See* e.g. page 3 lines 9-11 of Applicant's specification).

In contrast to the claimed invention, conventional systems are provided with a fixed interface and fixed protocols for communication between the secure device and the content player, which disadvantageously results in the content player only being usable with one or more specific secure devices (*See e.g.* page 1 lines 18-22 of Applicant's specification). Consequently,

[1] *See* Applicant's response electronically filed on June 21, 2007 in this application in response to the Final Office Action mailed March 21, 2007.

a (future) non-specified secure device requiring another protocol for communicating with a content player cannot be used in the conventional system.

The system disclosed by Graunke is to be considered a conventional system with respect to the above mentioned advantage of the claimed invention and disadvantage of conventional systems.

In the Continuation Sheet of the Advisory Action,[2] the Examiner provides a preliminary response to the amended claims. Applicant disagrees with the provided argumentation, which is basically a repetition of the previous Office Action[3] with additional explanation on how the Examiner understands the matter. It is the Applicant's opinion that a main difference between Graunke and the subject matter of claims 1-15 is still to be found in the information on the protocol for communication between content player and secure device.

The following sections provide additional explanation about the invention of claims 1-15, focusing on the protocol information and the use thereof, and how claims 1-15 are distinguishable over Graunke.

3.1) -- ***Where to find the protocol information.***

3.1.1) Claim 1 defines a control device for providing a protected contents structure.

3.1.2) The protected contents structure comprises (among others) attribute data and protocol information.

3.1.3) The attribute data is used to find relevant parts inside the protected contents structure. In other words, the attribute data is used to find the protocol information within the protected contents structure. The found protocol information is called information on the appropriate protocol.

3.2) -- ***What is the purpose of the protocol information.***

[2] *See* the Advisory Action mailed July 10, 2007 in this application.
[3] *See* the Final Office Action mailed March 21, 2007 in this application.

3.2.1) As defined in claim 1, the information on the appropriate protocol is used for establishing a communication interface between the content player and the secure device.

3.2.2) The communication interface is used for the secure device to transform secure device data communicated to the secure device through the communication interface into information required to decrypt the encrypted data.

In other words, this feature provides that:

- the communication interface is used to communicate secure device data from the content player to the secure device; and
- in the secure device, the secure device data is transformed into information required to decrypt the encrypted data.

3.2.3) Thus, the protocol information is directly related to the communication interface between content player and secure device. The aim of the invention of claims 1-15 is therefore formulated as "to provide systems and a method allowing to create a variable interface between secure device and content player." (*See e.g.* page 1, lines 23-25 of Applicant's specification). This in contrast to known systems and methods wherein "a fixed interface and protocols for communication between secure device and content player is provided" (*See e.g.* page 1, lines 18-20 of Applicant's specification).

3.3) -- ***More details about the protocol information and the communication interface using the protocol information.***

3.3.1) The invention of claims 1-15 provides a variable interface platform, wherein any communication interface between a secure device and content player can be established (*See e.g.* page 3, lines 6-8 of Applicant's specification). This is achieved by providing information on the appropriate protocol, which enables that the devices do not need to be preconfigured for using a particular protocol for establishing the communication interface.

3.3.2) The information on the protocol can be provided as one or more secure device applets (*See e.g.* page 4, lines 24-27 of Applicant's specification). The main function of the secure device applet is to implement in the content player the protocol and format to communicate with the secure device (*See e.g.* page 5, lines 7-10 of Applicant's specification). In other words, it provides information about how to establish a communication interface with the secure device.

3.3.3) The secure device applet makes it possible to provide an interface between the secure device and the content player without specific knowledge beforehand of the protocol required by the specific secure device used (*See e.g.* page 5, lines 10-13 of Applicant's specification).

!! This does not mean that the secure device applet equals an interface !!

It just explains that with the information comprised in the applet it is possible to establish an interface between secure device and content player.

3.3.4) Keys to decrypt the encrypted contents need to be retrieved by the content player from the secure device (*See e.g.* page 5, lines 30-32 of Applicant's specification). In order to get the keys, the content player needs to communicate with the secure device. The content player does not know how to establish a communication interface, so it searches the attribute data to select a security device applet (*See e.g.* page 6, lines 2-3 of Applicant's specification). With the information in the applet (i.e. by downloading it and having it executed in a virtual machine), a communication interface is established between content player and secure device (*See e.g.* page 6, lines 5-9 of Applicant's specification). Now secure device data can be send to the secure device, where the keys are obtained from the secure device data. The obtained keys can then be sent from the secure device to the content player via the established communication interface.

4) ***The following sections further discusses the Graunke Patent.***

4.1) -- ***Protocol information versus interface .***

4.1.1) The Examiner argues that the key module 'meets the recitation' of "protocol information".

4.1.2) The Examiner also uses the key module as equivalent of applet or plug-in or interface.

4.1.3) This already indicates that the invention is not correctly understood. Protocol information and communication interface are not the same. The protocol information of the invention of claims 1-15 is used to establish a communication interface.

4.2) -- ***Interpretation of key module.***

4.2.1) According to the Examiner the key module (protocol information) is for communication between the trusted player (content player) and the storage medium (secure device). Applicant's opinion this is not a correct interpretation of Graunke.

4.2.2) According to Graunke, the key is not nakedly transmitted to the trusted player, but wrapped into a key module (*See e.g.* column 4, lines 2-6 in Graunke). Thus, the key module contains keys. This is more related to secure device data then to protocol information, when comparing it to the invention of claims 1-15.

4.2.3) The key module can only be used by the right trusted player as determined by the key module (*See e.g.* column 4, lines 5-6 in Graunke). This has nothing to do with communication interfaces and protocols for communication interfaces, but is related to authorization.

4.2.4) The data on the storage medium is accessed by a program via the key module (*See e.g.* column 4, lines 35-37 in Graunke). Apparently the communication interface for accessing the storage medium is already present, i.e. it is fixed.

4.2.5) The key module ensures that the party requesting the decryption of an encrypted digital content is authentic and its integrity is verified (*See e.g.* column 4, lines 56-59 in Graunke). This is not related to establishing communication interfaces nor to protocol information to establish a communication interface.

4.3) -- ***Integrity and authenticity are main aspects of Graunke.***

4.3.1) The IVK is software that verifies that a program image corresponds to the supplied digital signature. It ensures that the program is not tampered with. (*See e.g.* column 5, lines 15-43 in Graunke). This is not related to the claimed invention.

4.3.2) The manifest is a statement of the integrity and authenticity (i.e. a signature) of the trusted player software (*See e.g.* column 6, lines 46-57 in Graunke). This is not related to the claimed invention.

4.3.3) When a user desires to view the encrypted content, the trusted player requests the keys required to perform decryption from key control software via lines 47 and 49 (*See e.g.* column 7, lines 16-20 in Graunke). Apparently these communication interfaces are fixed, thus this is not related to the claimed invention.

4.3.4) The key module generates the key module containing keys and code to validate the trusted player and an IVK (*See e.g.* column 7, lines 31-34 in Graunke). Thus, the key module does not comprise protocol information for establishing a communication interface. The key module is related to keys and authentication.

4.3.5) The key module is forwarded over communications network to client (*See e.g.* column 7, lines 40-41 in Graunke). Apparently the communication interfaces to do so are fixed.

4.3.6) The key module is generated to work with a specific trusted player as identified by the user's request and manifest (*See e.g.* column 7, lines 43-45 in Graunke). This is related to authenticity and is not related to the claimed invention.

4.3.7) The description of fig .4 is similarly related to validation and authenticity and is not related to the claimed invention.

4.4) -- ***Where are the keys decrypted.***

4.4.1) As noted by the Examiner, in Graunke the key module is arranged to transform encrypted keys into decrypted keys. Thus this is not done by the storage medium.

4.4.2) This invalidates the argument made by the Examiner that the storage medium can be seen as equivalent to the secure device. According to claim 1 of the invention, the keys are obtained by the secure device.

In summary Applicant does not find in Graunke the use of protocol information for establishing a communication interface.

Moreover, Applicant does not find in Graunke that the communication interface is used to communicate secure device data from the content player to the secure device.

Moreover, Applicant does not find in Graunke that in the secure device the secure device data is transformed into information required to decrypt the encrypted data.

Graunke is related to authenticity of devices and is not related to establishing communication interfaces.

For at least the reasons stated above, claims 1-15 are not anticipated by Graunke. Applicant respectfully requests reconsideration and withdrawal of the 35 U.S.C. § 102 rejection, and allowance of claims 1-15 as now pending in the application.

Reservation of Rights

In the interest of clarity and brevity, Applicant may not have addressed every assertion made in the Final Office Action. Applicant's silence regarding any such assertion does not constitute any admission or acquiescence. Applicant reserves all rights not exercised in connection with this response, such as the right to challenge or rebut any tacit or explicit characterization of any reference or of any of the present claims, the right to challenge or rebut any asserted factual or legal basis of any of the rejections, the right to swear behind any cited reference such as provided under 37 C.F.R. § 1.131 or otherwise, or the right to assert co-ownership of any cited reference. Applicant does not admit that any of the cited references or any other references of record are relevant to the present claims, or that they constitute prior art. To the extent that any rejection or assertion is based upon the Examiner's personal knowledge, rather than any objective evidence of record as manifested by a cited prior art reference, Applicant timely objects to such reliance on Official Notice, and reserves all rights to request that the Examiner provide a reference or affidavit in support of such assertion, as required by MPEP § 2144.03. Applicant reserves all rights to pursue any cancelled claims in a subsequent patent application claiming the benefit of priority of the present patent application, and to request rejoinder of any withdrawn claim, as required by MPEP § 821.04.

CONCLUSION

Applicant respectfully submits that the claims are in condition for allowance and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney 408-278-4042 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

Respectfully submitted,

WILHELMUS GERARDUS PETRUS MOOIJ

By his Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402
408-278-4042

Date AUGUST 21/2007 By Robert B. Madden
Robert B. Madden
Reg. No. 57,521

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being filed using the USPTO's electronic filing system EFS-Web, and is addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 21st, day of August, 2007.

Dawn R. Shaw
Name

Dawn Shaw
Signature